UNITED STATES DISTRICT COURT

DISTRICT OF MASSACHUSETTS

JONATHAN ROACH, individually and on behalf of all others similarly situated, Plaintiff, v. SHIELDS HEALTH CARE GROUP, INC., Defendant.	Civil Action No.: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Jonathan Roach ("Roach") ("Plaintiff"), on behalf of himself and all others similarly situated, by and through his undersigned counsel, brings this action against Shields Health Care Group, Inc. ("Shields Health" or "Defendant"). Plaintiff alleges as follows upon personal knowledge of the facts pertaining to himself, and on information and belief as to all other matters.

I. SUMMARY OF THE ACTION

1. In a statement posted on the Company's website on or about June 7, 2022, Shields Health admitted that between March 7, 2022, through March 21, 2022, its medical facilities and computer systems were hacked. The hackers intentionally attacked Shields Health to unlawfully access the highly sensitive, confidential, and personal information included in health and medical records of as many as two million of the Company's patients. Shields Health further acknowledged that this data breach (the "Shields Health Data Breach"), exposed and enabled the hackers to access the following Personal Identifying Information and Personal Health Information: names, Social Security numbers, dates of birth, billing information, home addresses, provider information, patient medical diagnosis, health insurance numbers and information, medical record numbers, patient IDs, and other medical or treatment information (hereinafter, the "PII" and "PHI").

2. Despite identifying the Shields Health Data Breach internally as early as March 18, 2022, Defendant waited more than two months before they began notifying consumers – patients of Shields Health – commencing on June 7, 2022, that the Shields Health Data Breach had occurred and that the sensitive PII and PHI of 2 million consumers may have been exposed.

3. Plaintiff brings this action on behalf of himself and a class of consumers defined herein (the "Class") as the members of which (the "Class Members") whose PII and PHI was disclosed to unauthorized third persons as a result of the Shields Health Data Breach.

II. PARTIES

4. Plaintiff Jonathan Roach is a citizen and resident of Massachusetts. Mr. Roach was the patient of Shields Health facility partners, Baystate Franklin MRI Center located within Baystate Franklin Medical Center in Greenfield, Massachusetts and at Baystate MRI and Imaging

in Springfield, Massachusetts, among others. He learned of the Shields Health Data Breach through a notice posted on the Shields Health's website. As a result of the Shields Health Data Breach, Mr. Roach has taken steps to secure his PII, including monitoring bank statements, credit card statements, and other financial information.

5. Defendant Shields Health Care Group, Inc., is a for-profit Massachusetts corporation and health care provider, which provides, among other things, MRIs, PET/CT scans, and "Ambulatory Surgical Services" for patients. Shields Health's principal place of business is located at 700 Congress Street, Suite 204, Quincy, Massachusetts 02169.

III. JURISDICTION AND VENUE

6. This Court has original jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2), because the matter in controversy, exclusive of interest and costs, exceeds the sum value of $5,000,000.00, consists of putative class membership of greater than 100 members, and is a class action in which some of the members of the Class, including the Plaintiff, are citizens of states different than that of Defendant.

7. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because Defendant is authorized to conduct business within this District, is headquartered in this District, has intentionally availed itself of the laws in this District, and conducts substantial business, including acts underlying the allegations of this complaint, in this District.

IV. FACTUAL ALLEGATIONS

A. Shields Health – A Provider of Medical and Health Related Services

8. Shields Health provides management and imaging services for more than 40 health care facilities throughout the New England area, including locations in Massachusetts, Maine and New Hampshire. It is regarded as the largest network of MRI centers in New England.[1]

[1] Shields Health Care Group, *Our Services*, available at https://shields.com/our-services/overview/ (last accessed June 28, 2022).

9. Patients utilizing Shields Health receive various health care services which include radiation oncology, PET/CT scans, MRIs and Ambulatory Searchable Center services.[2]

10. The procedures and protocols at Shields Health Group are – like virtually all other health care providers – established such that patients who receive its medical services or treatment must provide it with confidential personal and private information that includes their name and address; date of birth; highly confidential Social Security Numbers; their highly confidential and personal individual medical history; insurance information and coverage; information that relates to their doctor, nurse and other health care providers, and certain other information that may be necessary or required for the receipt of appropriate health care.

11. In the course of providing its medical services, Shields Health often gathers medical information about its patients, creates records (including medical record numbers, patient IDs and other medical or treatment information) with regard to the services it provides to them, and obtains personal confidential and private information from other entities, that form the Plaintiff's universe of health care providers including names of referring physicians, other doctors they may have seen, plaintiff's health plans and even, in many instances, the names of friends and family members.

12. From the outset of each patient's and Class Member's receipt of services from Shields Health, the Company represents and assures them that "Shields takes the confidentiality, privacy and security of information in our care seriously."[3]

13. In a further effort to assure patients that Shields Health Care is doing all that is necessary and required to protect the confidentiality of their personal medical information, the company adopted protocols and practices that it represents to patients are followed with respect to their Private Information (the "Privacy Practice").[4] This so-called Privacy Practice is included on Defendant's website. Importantly, the Privacy Practice is provided to every patient before they

---

[2] Shields Health Care Group, *Our Services*, *id.* (last accessed June 28, 2022).

[3] Shields Health Care Group, notice of data security incident, available at https://shields.com/notice-of-data-security-incident/ .(last accessed June 28, 2022).

[4] *See* Shields Health Care Group, *Privacy*, available at https://shields.com/privacy (last accessed June 23, 2022).

even receive treatment, because Shields Health is and should be mindful that those patients are providing to it their highly confidential and private information as discussed above.

14. Defendant makes a critically important representation in its Privacy Practice provided to each patient prior to treatment. Therein, Shields Health states that it "will generally only disclose health information about [patients] for the purposes of treatment, payment or health care operations." It further represents in its Privacy Practice that it will "[m]aintain the privacy of your health information as required by law."[5] And Shields Health expressly represents to every patient, including Plaintiff, the fact that it is required to "abide by the terms of this [Privacy Practice].[6]

15. Each Class Member, including the Plaintiff, received such Privacy Practice representations prior to receiving health related services from Defendant after which they entrusted Shields Health with their Private Information, and thereafter received such services from the Company.

B. The Occurrence of Each Breach and Failure to Timely Disclose the Shields Health Data Breach Harming Class Members

16. As Shields Health now acknowledges, between March 7, 2022 and March 21, 2022, an unknown party or entity breached its IT system, enabling that party or entity to access the PII and PHI of at least as many as 2 million Class Members.

The March 7, 2022 to March 21, 2022 Cyber-Attack

17. At all times material, Plaintiff and Class Members had a reasonable expectation that their PII and PHI were being safeguarded by Shields Health against disclosure to third parties, whether intentional or unintentional, directly or indirectly, and any exfiltration of that information. Unbeknownst to Plaintiff and Class Members, from approximately March 7, 2022 to March 21, 2022 – a period of two weeks – Shields Health was experiencing a targeted cyber security invasion by cyber thieves who had gained unauthorized access to its network. Further, Plaintiff and Class

[5] *Id.*
[6] *Id.*

Members did not know that Shields Health was in the process of investigating a data security alert at least as early as March 18, 2022.[7]

18. Unquestionably, Shields Health was a soft target for cyber thieves who recognized that as a health care entity it collects, maintains and even creates both PII and PHI. The cyber-attack was designed to and did gain access to such private and confidential data, including, *inter alia*, the PII and PHI of patients such as Plaintiff and Class Members.

19. According to Shields Health, cyber criminals accessed patient files that included names, address, dates of birth, Social Security numbers, patient ID numbers, insurance information, and/or medical information related to care received.[8] The cyber-attack was the result of inadequate security precautions and resulted in the exposure of PII and PHI of about 2 million patients. Shields Health has acknowledged this number.[9]

20. Despite knowing of the Shields Health Data Breach incident as early as March 18, 2022, and despite its obligations to provide adequate and timely notice so that affected persons can take precautions and mitigate potential losses and damages, Shields Health dropped the ball, initially put its head in the sand, and, ultimately realizing that the problem was serious and would not go away, belatedly published a press release regarding the Shields Health Data Breach on June 7, 2022, more than two months after the breach, in which it stated that the information accessed by cyber thieves included:

> Full name, Social Security number, date of birth, home address, provider information, diagnosis, billing information, insurance number and information, medical record number, patient ID and other medical or treatment information.[10]

21. Shields Health did not provide any notice to Plaintiff or Class Members at any time prior to June 7, 2022.

---

[7] Shields Health Care Group, *Notice of Data Security Incident* available at https://shields.com/notice-of-data-security-incident/ (last accessed June 23, 2022).

[8] *Id.*

[9] Associated Press, *Data Breach at Health Care Organizations May Affect 2 million*, available at https://apnews.com/article/technology-health-us-department-of-and-human-services-boston-massachusetts-4aed357bc7f3fd0a8a88f40d13985fdf(last accessed June 28, 2022).

[10] Shields Health Care Group, *Notice of Data Security Incident*, available at https://shields.com/notice-of-data-security-incident/(last accessed June 28, 2022).

22. The type of information that was secured by the cyber thieves reflects that this cyber-attack was targeted against Shields Health, given that it is a health care company.

23. The Shields Health Data Breach was clearly foreseeable to Defendant. It is well known, and is further alleged below, that cyber-attacks against health care organizations such as Defendant are targeted and frequent. Such data breaches against the health care sector have become widespread.

24. Given the fact that this was a targeted data breach against a health care company, it was foreseeable to Shields Health that the compromised PII and PHI could be used by hackers and cyber criminals in a variety of different ways. For example, PII and PHI can be used to identify or trace an individual's identity including the names, Social Security numbers and medical records either alone or in combination with other personal or identifying information that is connected or linked to an individual which could include ones birthplace, birth date, and mother's maiden name. Cyber criminals, who now possess class members PII and PHI, can readily obtain their tax returns or open fraudulent credit card accounts in their names. Shields Health was conscious of and could foresee the risk of data breaches given its position as a health care provider and the well documented and reported data breaches that have occurred throughout the medical industry over a number of years, with increasing frequency.

25. The increased frequency of data breaches has even captured the attention of the Federal Bureau of Investigation and the U.S. Secret Service. Both of whom have issued warnings to potential targets.

26. Defendant acknowledges that the Shields Health Data Breach occurred between March 7, 2022 and March 21, 2022, meaning that hackers had access to its systems, and consumers' data, for as many as fourteen (14) days.

27. Shields Health's dithering between March 18, 2022 and June 7, 2022 further prejudiced consumers who could have been taking affirmative steps to protect themselves from identity theft during that period of delay, and effectively prevented consumers from taking steps

to better or more timely insulate themselves from the risk of harm caused by misuse of their PII and PHI by hackers.

28. Just as it was aware of the substantial efforts made by hackers to attack health care providers, Defendant was aware that, for consumers, time is of the essence in dealing with the fallout from a breach that exposes their PII. Once a consumer's data has been compromised, there are numerous steps that they can take to protect themselves, as noted, for example, in an article on personal cybersecurity, a bank provides a list of affirmative steps to be taken after a consumer's data is compromised:

> **7 STEPS TO TAKE AFTER YOUR PERSONAL DATA IS COMPROMISED ONLINE**
>
> Unfortunately, data breaches have become a common feature of modern life in our always-connected world of online services; everyone in the U.S. is at risk of having their data stolen. However, even if your data is compromised in a data breach, you don't have to become a victim. There are several steps you can take to contain the damage and keep your personal finances, credit score, and identity safe from criminals.
>
> If you find out that a company you do business with – or an online service that you use – has suffered a data breach, here ***are a few steps to take right away***:
>
> **1. Change your passwords**
>
> It's a good idea to keep changing your password on a regular basis, but ***in the aftermath of a data breach, it's especially important to change your passwords to something strong***, secure, and unique. And you should have multiple "passwords," not just one. Do not use the same password for all of your online accounts. In general a "strong" password is at least 8 characters with a mixture of letters, numbers, and symbols. Consider using a password manager to help generate and keep track of your passwords.
>
> **2. Sign up for two-factor authentication**
>
> In addition to changing your passwords, sign up for two-factor authentication (also known as "2FA" or "two-step verification") wherever possible. This is an added layer of security for your account logins, and many services such as Gmail and Facebook now offer it. With two-factor authentication, your online account will require you to enter an additional level of identification to access your account – such as a code texted to your phone. This means that even if hackers get your email and password, they can't get into your account without that second factor of identity verification.
>
> **3. Check for updates from the company**
>
> If your data is involved in a major data breach, the company will likely post ongoing updates and disclosures about which customers were affected. For example, after a recent Facebook data breach, the company automatically logged out the users whose accounts were affected and sent them messages via the platform about what had happened and what

to do next. After the Equifax data breach, the Federal Trade Commission (FTC) offered a series of advisories and steps that people could take to protect themselves.

4. Watch your accounts, check your credit reports

After a data breach, ***it's essential to be vigilant and pay extra attention to your account activity – that includes your account at the company that suffered the breach, as well as your bank account and other financial accounts***. Read your credit card statements and watch for suspicious transactions. Also, sign up for your free annual credit report to check your credit reports from each of the three credit reporting bureaus.

5. Consider identity theft protection services

If you want additional peace of mind, you can consider signing up for identity theft protection services. However, these services are not cheap, and you can do many of the actions yourself. Often when there is a significant data breach, the company involved will give affected customers a free year of credit monitoring.

6. Freeze your credit

Another step you can take, whether you're affected by a data breach or not, is to freeze your credit. You can do this by contacting each of the three credit bureaus (Equifax, Experian, and TransUnion) and asking to freeze your credit. There is no cost to freeze your credit, and it will prevent any new credit accounts from being opened in your name. Even if identity thieves have access to all of your personal data, they can't open new accounts under your name if your credit is frozen. The only drawback of freezing your credit is that it prevents you from applying for new credit too – so don't do it if you are expecting to need a new car loan, home loan, or credit card account. You can un-freeze your credit at any time.

7. Go to IdentityTheft.gov

If you are affected by a data breach, there is a government website that can help you assess the situation and understand your options for what to do next. There are a variety of resources with tips and advice on what to do if your personal information was lost or stolen.

Being affected by a data breach can be alarming, and in the worst-case scenario, it can lead to identity theft and financial complications. But if you know what to expect, and you take a few simple steps to protect yourself and stay vigilant, you can overcome the risks and hassles of a data breach.[11]

Of course, with a data breach, knowledge is power and here, for more than 2 months after Defendant discovered the Shields Health Data Breach, it hid its existence and extent from Plaintiff and Class Members, consumers and patients, whose data was entrusted to Defendant and whose data, by law, it is required to protect.

[11] https://www.fultonbank.com/Education-Center/Privacy-and-Security/personal-data-breach-tips, last visited June 28, 2022.

C. Medical Records Are Uniquely Valuable to Hackers

29. Medical Records are uniquely valuable to hackers. Indeed, they prey on medical/health care entities. And health care providers, such as Shields Health, have been aware of this for a number of years as well as the need to take adequate measures to secure their systems and information. In 2018 alone, over 400 breaches targeting medical data were reported to the Inspector General of the Department of Health and Human Services.[12] That figure represented a substantial increase from the year before. The steady growth of hacks of healthcare entities is no surprise and can be tied to two significant factors, (1) the failure of healthcare entities, like Shields Health, to adequately protect patient data and (2) the substantial value of medical records, which include a broad range of PII and PHI. The high value placed on medical records is, according to the head of investigations at the HHS Office of Inspector General, a reflection of the "treasure trove" of data contained within them.[13]

30. The continued vulnerability of the health care industry to hacking is widely recognized within the health care industry. An article published on the website of Advisory Board, a company that advises health care providers, health insurance companies and others on issues critical to the health care industry, recognized that "the cyber threats we face are growing in sophistication and magnitude and becoming more difficult to combat."[14] The article further noted that "[a]s a result, every health care organization needs to have a strong strategy in place to mitigate cyber risk."

31. Large health care providers like Shields Health are well aware of the risks data breaches pose to their patients, especially because both the size of their patient base and the fact that the PHI and PII that they collect and maintain from their patients is profoundly valuable to hackers. A 2017 survey by Accenture determined that 50% of healthcare data breach victims eventually suffered medical identity theft, resulting in an average of $2,500 in out of pocket costs

---

[12] https://www.cbsnews.com/news/hackers-steal-medical-records-sell-them-on-dark-web/ and https://www.advisory.com/en/daily-briefing/2019/03/01/hackers (last visited on June 23, 2022).

[13] https://www.cbsnews.com/news/hackers-steal-medical-records-sell-them-on-dark-web/, (last visited on June 23, 2022).

[14] https://www.advisory.com/en/daily-briefing/2019/03/01/hackers, (last visited on June 23, 2022).

per patient.[15] That same survey also highlighted the importance of rapid disclosure of healthcare data breaches as it noted that "half of the survey respondents reported that they learned of the breach themselves – as opposed to an official company or law enforcement notification – after they had been alerted to an error on their benefits explanation, credit card statement, or similar documents."[16] Even where hacked healthcare data is not used to steal identities, its theft poses substantial harm to consumers. In February 2021, hackers published "extensive" patient information hacked from two U.S. hospital groups in an extortion effort.[17] The hackers made off with "tens of thousands of files containing patients' personal medical information" from just eleven hospitals.[18] In that breach, detailed medical data was posted, unencrypted, on the dark web including "at least tens of thousands of scanned diagnostic results and letters to insurers. One folder contains background checks on hospital employees. An Excel document titled 2018_colonoscopies has 102 full names, dates and details of the procedures, and a field to mark "yes" or "no" to whether the patient has a 'normal colon.'"[19] Such public posting of confidential PHI and PII is part of a trend to extort money from health care providers and/or individual patients, posting detailed medical records and other PII or PHI if victims refuse to pay.

D. Shields Health's Failure to Protect Consumer PHI is a Violation of HIPPA

32. Health care providers such as Shields Health are bound by the HIPPA Privacy Rule, 45 CFR §§ 160, 164, which protects all "*"individually identifiable health information,"* or PHI "held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral." PHI includes:

---

15 Top 10 Biggest Healthcare Data Breaches of All Time | Digital Guardian, (last visited on June 28, 2022).

16 *Id.*

17 https://www.nbcnews.com/tech/security/hackers-post-detailed-patient-medical-records-two-hospitals-dark-web-n1256887, last visited on June 28, 2022.

18 https://hacked.com/hackers-medical-records/, last visited on June 28, 2022.

19 Hackers post detailed patient medical records from two hospitals to the dark web (nbcnews.com), last visited on June 28, 2022.

> . . . information that is a subset of health information, including demographic information collected from an individual, and:
>
> > (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
> >
> > (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
> >
> > > (i) That identifies the individual; or
> > >
> > > (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

45 CFR § 160.103. The privacy rule requires that covered entities, including health care providers like Shields Health, provide sufficient safeguards to protect the privacy of the PHI entrusted to them by patients. Entities covered by the HIPPA Privacy Rule are required to report breaches of unsecured health information to the Secretary of Housing and Human Services ("HHS") as soon as possible after discovery of the breach. 45 CFR § 164.408. Here, Plaintiff is informed and believes and thereon alleged that if Shields Health reported the breach to HHS, it was no earlier than June 7, 2022. Shields Health did not report the breach to HHS until no earlier, the same day that Defendant publicly acknowledged the Shields Health Data Breach, despite acknowledging that they initially discovered a possible data breach.

V. CLASS ALLEGATIONS

33. Pursuant to Fed. R. Civ. P. 23(b)(1), (b)(2), (b)(3), and (c)(4), Plaintiff asserts common law claims for negligence (Count I), negligence per se (Count II), breach of implied contract (Count III), breach of the implied covenant of good faith and fair dealing (Count IV), negligent misrepresentation (Count V), invasion of privacy (Count VI), breach of fiduciary duty (Count VII) and unjust enrichment (Count VIII), on behalf of the following Class (collectively "the Class"), defined as follows:

Nationwide Class: All residents of the United States whose PII or PHI was accessed or otherwise compromised as a result of the Shields Health Data Breach.

Massachusetts Class: All residents of the state of Massachusetts whose PII or PHI was accessed or otherwise compromised as a result of the Shields Health Data Breach.

Members of the Nationwide Class and the Massachusetts Class are referred to herein collectively as "Class Members" or "Class."

34. Excluded from the Class are Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and the members of their immediate families and judicial staff.

35. The proposed Class meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

36. **Numerosity**: The exact number of members of the Class is unknown to Plaintiff at this time but Shields Health operates approximately 114 medical centers in twenty-one states, employing several hundred board-certified dermatologists, moreover, in its report to HSS, Shields Health acknowledged that the number of "Individuals Affected" by the Shields Health Data Breach was 2,413,553, indicating that there are more than 2.4 million members of the Nationwide Class, making joinder of each individual impracticable. Moreover, Shields Health operates several locations in Massachusetts, New Hampshire, and Rhode Island, suggesting that there are thousands of members of the Class, making joinder of each individual impracticable. Ultimately, members of the Class will be easily identified through Defendant' records.

37. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a) Whether Defendant failed to adequately safeguard Plaintiff's and the Class Members' PII and PHI;

b) Whether Defendant failed to protect Plaintiff's and the Class Members' PII and PHI, as promised;

c) Whether Defendant' computer system systems and data security practices used to protect Plaintiff's and the Class Members' PII and PHI violated HIPAA, federal, state and local laws, or Defendant' duties;

d) Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiff's and the Class Members' PII and PHI properly and/or as promised;

e) Whether Defendant violated the consumer protection statutes, data breach notification statutes, state unfair insurance practice statutes, state insurance privacy statutes, and state medical privacy statutes applicable to Plaintiff and each of the Class;

f) Whether Defendant failed to notify Plaintiff and members of the Class about the Shields Health Data Breach as soon as practical and without delay after the Shields Health Data Breach was discovered;

g) Whether Defendant acted negligently in failing to safeguard Plaintiff's and the Class Members' PII and PHI;

h) Whether Defendant entered into contracts with Plaintiff and the Class Members that included contract terms requiring Defendant to protect the confidentiality of Plaintiff's PII and PHI and have reasonable security measures;

i) Whether Defendant' conduct described herein constitutes a breach of its contracts with Plaintiff and the members of each of the Class;

j) Whether Defendant should retain the money paid by Plaintiff and members of each of the Class to protect their PII and PHI;

k) Whether Plaintiff and the Class Members are entitled to damages as a result of Defendant' wrongful conduct;

l) Whether Plaintiff and the Class Members are entitled to restitution as a result of Defendant's wrongful conduct;

m) What equitable relief is appropriate to redress Defendant's wrongful conduct; and

n) What injunctive relief is appropriate to redress the imminent and currently ongoing harm faced by Class Members.

38. **Typicality**: Plaintiff's claims are typical of the claims of the members of the Class. Plaintiff and the Class Members sustained damages as a result of Defendant's uniform wrongful conduct during transactions with them.

39. **Adequacy**: Plaintiff will fairly and adequately represent and protect the interests of the Class and has retained counsel competent and experienced in complex litigation and class actions. Plaintiff has no interests antagonistic to those of the Class, and there are no defenses unique to Plaintiff. Plaintiff and his counsel are committed to prosecuting this action vigorously on behalf of the members of the proposed Class and have the financial resources to do so. Neither Plaintiff nor his counsel have any interest adverse to those of the other members of the Class.

40. **Risks of Prosecuting Separate Actions**: This case is appropriate for certification because prosecution of separate actions would risk either inconsistent adjudications which would establish incompatible standards of conduct for the Defendant or would be dispositive of the interests of members of the proposed Class. Furthermore, the Shields Health Database still exists, and is still vulnerable to future attacks – one standard of conduct is needed to ensure the future safety of the Shields Health Database.

41. **Policies Generally Applicable to the Class**: This case is appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Plaintiff and proposed Class as a whole, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct towards members of the Class and making final

injunctive relief appropriate with respect to the proposed Class as a whole. Defendant's practices challenged herein apply to and affect the members of the Class uniformly, and Plaintiff's challenge to those practices hinges on Defendant's conduct with respect to the proposed Class as a whole, not on individual facts or law applicable only to Plaintiff.

42. **Superiority**: This case is also appropriate for certification because class proceedings are superior to all other available means of fair and efficient adjudication of the claims of Plaintiff and the members of the Class. The injuries suffered by each individual member of the Class are relatively small in comparison to the burden and expense of individual prosecution of the litigation necessitated by Defendant's conduct. Absent a class action, it would be virtually impossible for individual members of the Class to obtain effective relief from Defendant. Even if Class Members could sustain individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties, including the Court, and would require duplicative consideration of the common legal and factual issues presented here. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single Court.

VI. CAUSES OF ACTION

COUNT I – NEGLIGENCE

43. Plaintiff incorporates the above allegations by reference.

44. Defendant required Plaintiff and Class Members to submit PII and PHI in order to obtain insurance coverage and/or to receive health care services.

45. Defendant knew, or should have known, of the risks inherent in collecting and storing the PII and PHI of Plaintiff and Class Members.

46. As described above, Shields Health owed duties of care to Plaintiff and Class Members whose PII and PHI had been entrusted with Shields Health.

47. Defendant breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII and PHI.

48. Defendant acted with wanton disregard for the security of Plaintiff and Class Members' PII and PHI. Defendant knew or should have known that Shields Health had inadequate computer systems and data security practices to safeguard such information, and Defendant knew or should have known that hackers were attempting to access the PII and PHI in health care databases, such as Shields Health's.

49. A "special relationship" exists between Defendant and the Plaintiff and Class Members. Shields Health entered into a "special relationship" with Plaintiff and Class Members because Shields Health collected the Personal Identifying Information of Plaintiff and the Class Members and stored it in the Shields Health Database – information that Plaintiff and the Class Members had been required to provide to Shields Health.

50. But for Defendant's wrongful and negligent breach of the duties owed to Plaintiff and the Class Members, Plaintiff and the Class Members would not have been injured.

51. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known it was failing to meet its duties, and that Defendant's breach would of such duties cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their PII and PHI.

52. As a direct and proximate result of Defendant' negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II – NEGLIGENCE *PER SE*

53. Plaintiff incorporates the above allegations by reference.

54. Pursuant to the Federal Trade Commission Act (15 U.S.C. §45), Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII and PHI.

55. Pursuant to HIPAA (42 U.S.C. §1302d et. seq.), Defendant had a duty to implement reasonable safeguards to protect Plaintiff's and Class Members' PII and PHI.

56. Defendant breached its duties to Plaintiff and Class Members under the Federal Trade Commission Act (15 U.S.C. § 45) and HIPAA (42 U.S.C. § 1302d *et. seq.*), by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard plaintiff's and Class Members' PII and PHI.

57. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

58. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

59. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their PII and PHI.

60. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT III – BREACH OF IMPLIED CONTRACT

61. Plaintiff incorporates the above allegations by reference.

62. Plaintiff and Class members entered into an implied contract with Shields Health when they obtained health care services from Shields Health, for which they were required to provide their PII and PHI. The PII and PHI provided by Class Members to Shields Health was governed by and subject to Shields Health's privacy duties and policies.

63. Shields Health agreed to safeguard and protect the PII and PHI of Plaintiff and Class Members and to timely and accurately notify them in the event that their PII or PHI was breached or otherwise compromised.

64. Plaintiff and Class members entered into the implied contracts with the reasonable expectation that Defendant's data security practices and policies were reasonable and consistent

with industry standards. Plaintiff and Class members believed that Shields Health would use part of the monies paid to Shields Health under the implied contracts to fund adequate and reasonable data security practices.

65. Plaintiff and Class members would not have obtained health care services from Shields Health or provided and entrusted their PII and PHI to Defendant in the absence of the implied contract or implied terms between them and Shields Health. The safeguarding of the PII and PHI of Plaintiff and Class Members and prompt and sufficient notification of a breach was critical to realize the intent of the parties.

66. Plaintiff and Class Members fully performed their obligations under the implied contracts with Shields Health.

67. Shields Health breached its implied contracts with Plaintiff and Class members to protect their PII and PHI when it (1) failed to have security protocols and measures in place to protect that information; (2) disclosed that information to unauthorized third parties; and (3) failed to provide timely and accurate notice that their PII and PHI was compromised as a result of the Shields Health Data Breach.

68. As a direct and proximate result of Shields Health's breaches of implied contract, Plaintiff and Class members sustained actual losses and damages as described in detail above and are also entitled to recover nominal damages.

COUNT IV – BREACH OF IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING

69. Plaintiff incorporates the above allegations by reference.

70. Plaintiff and Class Members entered into valid, binding, and enforceable express or implied contracts with Shields Health, as alleged above.

71. These contracts were subject to implied covenants of good faith and fair dealing that all parties would act in good faith and with reasonable efforts to perform their contractual obligations (both explicit and fairly implied) and not to impair the rights of the other parties to receive the rights, benefits, and reasonable expectations under the contracts. These included the

implied covenants that Shields Health would act fairly and in good faith in carrying out its contractual obligations to take reasonable measures to protect plaintiff's PII and PHI and to comply with industry standards and federal and state laws and regulations.

72. A "special relationship" exists between Shields Health and the Plaintiff and Class Members. Shields Health entered into a "special relationship" with Plaintiff and Class Members who sought medical services or treatment at Shields Health facilities and, in doing so, entrusted Shields Health, pursuant to its requirements, with their PII and PHI.

73. Despite this special relationship with Plaintiff, Shields Health did not act in good faith and with fair dealing to protect plaintiff's and Class Members' PII and PHI.

74. Plaintiff and Class Members performed all conditions, covenants, obligations, and promises owed to Shields Health.

75. Shields Health's failure to act in good faith in implementing the security measures required by the contracts denied Plaintiff and Class Members the full benefit of their bargain, and instead they received health insurance and related services that were less valuable than what they paid for and less valuable than their reasonable expectations under the contracts. Plaintiff and Class Members were damaged in an amount at least equal to this overpayment.

76. Shields Health's failure to act in good faith in implementing the security measures required by the contracts also caused Plaintiff and Class Members to suffer actual damages resulting from the theft of their PII and PHI and remain at imminent risk of suffering additional damages in the future.

77. Accordingly, Plaintiff and Class Members have been injured as a result of Shields Health's breach of the covenant of good faith and fair dealing and are entitled to damages and/or restitution in an amount to be proven at trial.

COUNT V – NEGLIGENT MISREPRESENTATION

78. Plaintiff incorporates the above allegations by reference as fully set forth herein.

79. Defendant negligently and recklessly misrepresented material facts, pertaining to the provision of health care services, to Plaintiff and Class Members by representing that it would

maintain adequate data privacy and security practices and procedures to safeguard Plaintiff's and Class Members' PII and PHI from unauthorized disclosure, release, data breaches, and theft.

80. Defendant negligently and recklessly misrepresented material facts, pertaining to the provision of health care services, to Plaintiff and Class Members by representing that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiff's and Class Members' PII and PHI.

81. Because of multiple warnings about the inadequacy of its data privacy and security practices, Defendant either knew or should have known that its representations were not true.

82. In reliance upon these misrepresentations, Plaintiff and Class Members obtained health care services from Defendant.

83. Had Plaintiff and Class Members, as reasonable persons, known of Defendant's inadequate data privacy and security practices, or that Defendant was failing to comply with the requirements of federal and state laws pertaining to the privacy and security of Plaintiff's and Class Members' PII and PHI, he would not have purchased health services from Defendant, and would not have entrusted their PII and PHI to Defendant.

84. As direct and proximate consequence of Defendant's negligent misrepresentations, Plaintiff and Class Members has suffered the injuries alleged above.

COUNT VI – INVASION OF PRIVACY

85. Plaintiff incorporates the above allegations by reference.

86. Plaintiff and Class Members had a reasonable expectation that Defendant would maintain the privacy of the PII and PHI collected and maintained by Shields Health.

87. Shields Health represented to Plaintiff and Class Members that it would not disclose their PII and PHI except in a handful of clearly defined and disclosed circumstances.

88. Despite representations to the contrary, Defendant failed to protect and safeguard the PII and PHI entrusted to Shields Health by Plaintiff and Class Members and in so doing intruded on the private and personal affairs of Plaintiff and Class Members in a manner highly offensive to a reasonable person; invaded the privacy of Plaintiff and Class Members by disclosing,

without authorization, the PHI and PII of Plaintiff and Class Members, inconsistent with both the purpose of the collection of the PII and PHI and inconsistent with the uses of said PII and PHI previously disclosed to Plaintiff and Class Members; failed to provide sufficient security to protect the PII and PHI of Plaintiff and Class Members from unauthorized access; enabled, by failing to protect it sufficiently, the disclosure of PII and PHI without the consent of Plaintiff or Class Members.

89. Shields Health knew, or acted with reckless disregard in not knowing, that the PII and PHI collected from Plaintiff and Class Members was, because of its nature, subject to a significant risk of unauthorized access.

90. Shields Health knew, or acted with reckless disregard in not knowing, that a reasonable person would consider its failure to adequately protect and secure their PII and PHI to be highly offensive.

91. Shields Health's disclosure of Plaintiff's and Class Members' PII and PHI without their consent constituted a violation of the privacy of Plaintiff and Class Members.

92. Shields Health's failure to provide sufficient security to protect the PII and PHI of Plaintiff and Class Members, leading to unauthorized access to that data by unauthorized parties constituted the unlawful publication of that PII and PHI by Shields Health.

93. The PII and PHI disclosed in the Shields Health Data Breach was not generally known to the public and is not a matter of legitimate public concern.

94. Plaintiff and Class Members had a reasonable expectation in the privacy of the PII and PHI that they provided to Shields Health. That reasonable expectation was thwarted by Defendant actions and inactions and Defendant's conduct constituted an invasion of Plaintiff's and Class Members' privacy.

95. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial as well as restitution and injunctive relief.

COUNT VII – BREACH OF FIDUCIARY DUTY

96. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

97. Plaintiff brings this claim on behalf of himself and all members of the Classes.

98. Defendant accepted the special confidence placed in it by Plaintiff and Class Members, even asserting that it is "takes the confidentiality, privacy, and security of information in [its] care seriously" and by the promulgation of its Privacy Practice. There was an understanding between the parties that Defendant would act for the benefit of Plaintiff and Class Members in preserving the confidentiality of the Private Information.

99. Defendant became the guardian of Plaintiff's and the Class Members' Private Information and accepted a fiduciary duty to act primarily for the benefit of its patients, including Plaintiff and the Class Members, including safeguarding Plaintiff's and the Class Members' Private Information.

100. Defendant's fiduciary duty to act for the benefit of Plaintiff and Class Members pertains as well to matters within the scope of its medical relationship with its patients, in particular, to keep secure the Private Information of those patients.

101. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to (a) diligently discover, investigate, or give notice of the Data Breach in a reasonable and practicable period of time; (b) encrypt and otherwise protect the integrity of its computer systems containing Plaintiff's and the Class Members' Private Information; (c) timely notify and/or warn them of the Shields Health Data Breach; (d) ensure the confidentiality and integrity of electronic PHI Defendant created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1); (e) implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. § 164.312(a)(1); (f) implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1); (g) identify and respond to suspected or known security incidents and

to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 C.F.R. § 164.308(a)(6)(ii); (h) protect against any reasonably anticipated threats or hazards to the security or integrity of electronic PHI, in violation of 45 C.F.R. § 164.306(a)(2); (i) protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3); (j) ensure compliance with the HIPAA security standard rules by its workforce, in violation of 45 C.F.R. § 164.306(a)(94); (k) effectively train all members of its workforce (including independent contractors) on the policies and procedures necessary to maintain the security of PHI, in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); (l) design, implement, and enforce Case 1:22-cv-10901, Document 1, Filed 06/09/22, policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in violation of 45 C.F.R. § 164.530(c); and (m) by otherwise failing to safeguard Plaintiff's and the Class Members' Private Information.

102. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and/or Class Members have suffered and/or will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Shields Health Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Shields Health Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendant's services they received.

103. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT VIII – UNJUST ENRICHMENT

104. Plaintiff incorporates the above allegations by reference as fully set forth herein.

105. Plaintiff and Class Members conferred a monetary benefit on Defendant in the form of payments made for the purchase of health care services.

106. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiff and Class Members.

107. The payments for healthcare services that Plaintiff and Class Members paid (directly or indirectly) to Defendant should have been used by Defendant, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

108. As a result of Defendant's conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between the health care services with the reasonable data privacy and security practices and procedures that Plaintiff and Class Members paid for, and the inadequate health care services without reasonable data privacy and security practices and procedures that they received.

109. Under principals of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiff and Class Members paid for and that were otherwise mandated by HIPAA regulations, federal, state and local laws, and industry standards.

110. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds received by Defendant.

111. A constructive trust should be imposed upon all unlawful or inequitable sums received by Defendant traceable to Plaintiff and Class Members.

112. Plaintiff and Class Members have no adequate remedy at law.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Class Members, seek the following relief:

A. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointed the undersigned as Class counsel, and finding that Plaintiff is the proper representative of the Class requested herein.

B. Plaintiff requests injunctive relief. Awarding injunctive and other equitable relief as is necessary to protect the interests of the Class Members, including:

(i) an order prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

(ii) requiring Defendant to protect all data collected or received through the course of its business in accordance with HIPAA regulations, other federal, state and local laws, and best practices under industry standards;

(iii) requiring Defendant to design, maintain, and test its computer systems to ensure that PII and PHI in its possession is adequately secured and protected;

(iv) requiring Defendant to disclose any future data breaches in a timely and accurate manner;

(v) requiring Defendant to engage third-party security auditors as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis and ordering them to promptly correct any problems or issues detected by these auditors;

(vi) requiring Defendant to audit, test, and train its security personnel to run automated security monitoring, aggregating, filtering and reporting on log information in a unified manner;

(vii) requiring Defendant to implement multi-factor authentication requirements;

(viii) requiring Defendant's employees to change their passwords on a timely and regular basis, consistent with best practices;

(ix) requiring Defendant to encrypt all PII and PHI;

(x) requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

(xi) requiring Shields Health to segment data by, among other things, creating firewalls and access controls so that if one area of its network is compromised, hackers cannot gain access to other portions of its systems;

(xii) requiring Defendant to purge, delete, and destroy in a reasonably secure and timely manner PII and PHI no longer necessary for its provision of services;

(xiii) requiring Defendant to conduct regular database scanning and securing checks;

(xiv) requiring Defendant to routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

(xv) requiring Defendant to provide lifetime credit monitoring and identity theft repair services to members of the Class; and

(xvi) requiring Defendant to educate all Class Members about the threats they face as a result of the loss of their PII and PHI to third parties, as well as steps Class Members must take to protect themselves.

C. Plaintiff also requests actual damages, punitive damages, treble damages, statutory damages, exemplary damages, equitable relief, restitution, disgorgement of profits, attorney's fees, statutory costs, and such other and further relief as is just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

///

///

///

Dated: June 29, 2022

Respectfully submitted,

BERMAN TABACCO

/s/ Patrick T. Egan
PATRICK T. EGAN (BBO 637477)

NATHANIEL L. ORENSTEIN (BBO 664513)
One Liberty Square
Boston, MA 02109
Telephone: (617) 542-8300
pegan@bermantabacco.com
norenstein@bermantabacco.com

GEORGE GESTEN MCDONALD, PLLC
LORI G. FELDMAN*
102 Half Moon Bay Drive
Croton-on-Hudson, NY 10520
Telephone: (917) 983-9321
lfeldman@4-justice.com
eservice@4-justice.com

DAVID J. GEORGE*
9897 Lake Worth Road, Suite 302
Lake Worth, FL 33467
Telephone: (561) 232-6002
dgeorge@4-justice.com
eservice@4-justice.com